DETAILED ACTION

1. This action is in response to the amendment filed on 09/09/2009.

2. Claims 1-42 are pending for consideration.

Response to Arguments

3. Applicant's arguments, filed on 09/09/2009, with respect to claims 1-42 have been fully considered and are persuasive. The final rejection of claims 1-42 has been withdrawn.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Charles Li on 09/23/2009.

Claims 1 and 23 have been amended as follows:

Claim 1:

(Currently Amended) A network computer system for providing security, wherein the network computer system comprises:

at least one processor, at least one storage device, and at least one network interface device that are configured to implement:

a monitoring function for the network computer system;

at least one outside server for an untrusted computer network, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one outside server for the untrusted computer network;

at least one proxy server, wherein the at least one outside server for the untrusted computer network is able to read and write data to the at least one proxy server, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one proxy server;

at least one inside server, wherein the at least one proxy server is able to read and write data to the at least one inside server, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one inside server; and

a core operating system that is a portion of an operating system, wherein the at least one outside server, the at least one proxy server and the at least one inside server can read and execute data from, but cannot write data to, the core operating system.

Claim 23:

(Currently Amended) A network computer system for providing security, wherein the network computer system comprises:

at least one processor, at least one storage device, and at least one network interface device that are configured to implement:

at least one system level auditing function, wherein the at least one system level auditing function resides within a first compartment and the at least one system level auditing function transports system log protocol events produced by an operating system through the network computer system;

at least one intrusion detection system, wherein the at least one intrusion detection system resides within a second compartment and a third compartment, wherein the second compartment monitors activity and makes comparisons to known patterns that may indicate an attack on the network computer system and the third compartment is where source code for the intrusion detection system resides, wherein the second compartment can read and execute data from, but cannot write data to, the third compartment;

at least one system health monitoring tool, wherein the at least one system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fourth compartment monitors health and response time for the at least one outside server, the at least one proxy server and the at least one inside server and the fifth compartment is where source code for the system health monitoring tool resides, wherein the fourth compartment can read and execute data from, but cannot write data to, the fifth compartment;

at least one integrity check system, wherein the at least one integrity check system resides within a sixth compartment and a seventh compartment, wherein the sixth compartment will provide an integrity check function to monitor changes to a baseline configuration of the network computer system and the seventh compartment is where source code for the integrity check system resides, wherein the sixth compartment can read and execute the source code from, but cannot write data to, the seventh compartment;

at least one core operating system, residing within a fourteenth compartment;

at least one outside server for an untrusted computer system, wherein the outside server includes at least one eighth compartment where outside requests are received and processed and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from, but cannot write data to, the at least one core operating system that resides in the fourteenth compartment and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one outside server;

at least one proxy server, wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server and at least one eleventh compartment where source code for the at least one proxy server resides, wherein the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the at least one core operating system, residing in the fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one proxy server; and

wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all and requests received from the file unsecured computer network have been screened and deemed valid for further processing by the at least one proxy server and at least one thirteenth compartment where source code for the at least one inside server resides, wherein the at least one twelfth compartment can read and execute data from, but cannot write data to, the at least one thirteenth compartment and the at least one thirteenth compartment can read and execute data from, but cannot write data to, the at least one core operating system, residing in the fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one inside server.

Allowable Subject Matter

5. Claims 1-42 are allowed.

6. The following is an examiner's statement of reasons for allowance:

7. As noted above, the Examiner agrees with the Applicant's arguments on pages 22-28 of the Remarks, specifically that the prior arts do not teach the five elements recited in independent claims 1 and 26 "a monitoring function, at least one outside server, at least one proxy server, at least one inside server, and a core operating system". As for independent claims 23 and 40, the prior arts do not teach a first compartment through a fourteenth compartment which was used for providing security to computing systems. The Examiner was unable to find a teaching, suggestion, or motivation that would render the above limitation obvious. Claims 1-42 are, therefore, novel and not obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431